

Stephen A. Weiss
Christopher L. Ayers
SEAGER WEISS LLP
55 Challenger Road, 6th Floor
Ridgefield Park, New Jersey 07660
Telephone: (212) 584-0700
Facsimile: (212) 584-0799
E-mail: sweiss@seegerweiss.com
E-mail: cayers@seegerweiss.com

James E. Cecchi
Donald A. Ecklund
Michael A. Innes
CARELLA, BYRNE, CECCHI,
OLSTEIN, BRODY & AGNELLO, PC
5 Becker Farm Road
Roseland, NJ 07068-1739
(973) 994-1700
Email: jcecchi@carellabyrne.com
Email: decklund@carellabyrne.com
Email: minnes@carellabyrne.com

Attorneys for Plaintiffs

**UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY**

JAY MALKOFF and KENNETH IRVINE,
individually and on behalf of all others,

Plaintiffs,

v.

FACEBOOK INC., CAMBRIDGE ANALYTICA,
CAMBRIDGE ANALYTICA(UK) LTD.,
CAMBRIDGE ANALYTICA LLC, ROBERT
MERCER, and ALEKSANDR KOGAN

Defendants.

Civil Action No.:

**CLASS ACTION COMPLAINT
AND
DEMAND FOR JURY TRIAL**

Jay Malskoff and Kenneth Irvine (“Plaintiffs”), on behalf of themselves and all others similarly situated, on personal knowledge as to the facts concerning themselves, on information and belief as to all other matters, and based on the investigation of counsel and public statements, brings this class action against Facebook Inc. (“Facebook”), Cambridge Analytica(UK) Ltd. (“CA UK1”), Cambridge Analytica Ltd. (“CA UK2”), Cambridge Analytica LLC (“CA USA”), Robert Mercer (“Mercer”), and Aleksandr Kogan (“Kogan”) (collectively, CA UK1, CA UK2, and CA USA shall be referred to as “Cambridge Analytica” and together with Facebook, Mercer, and Kogan as the “Defendants”) and allege as follows:

NATURE OF ACTION

1. This action concerns a severe and unprecedented breach of trust committed by Defendants which allowed Cambridge Analytica to secretly and unlawfully harvest highly sensitive personal information of Facebook users.

2. Cambridge Analytica and its cronies conspired to improperly obtain personal profile data from nearly 50 million Facebook users without their consent or knowledge, including Plaintiffs and Class members, in excess of any authorization granted by Facebook and Facebook users.

3. Despite the fact that it was storing sensitive information, Facebook failed to protect and safeguard its users’ data and, upon learning of the unauthorized access and use of its users’ information, failed to take reasonable measures necessary to secure and destroy the data.

4. Facebook also failed to notify its users that their sensitive personal information had been harvested and misused when it learned of the unauthorized acquisition, and only spoke publicly on the issue after news stories exposed their negligent behavior.

5. In March 2018, a whistleblower and former contractor with Cambridge Analytica,

Christopher Wylie, revealed how Cambridge Analytica – a company owned by the hedge fund billionaire Robert Mercer, and headed at the time by Steve Bannon, President Trump’s key adviser and former chief political strategist – harvested and used personal information taken without authorization from millions of Facebook users’ profiles in early 2014 to build a system that could profile individual U.S. voters, in order to target them with personalized political advertisements and influence choices at the ballot box.

6. Wylie, who worked with Aleksandr Kogan, a Cambridge University academic, to obtain the data, stated: “[Cambridge Analytica] exploited Facebook to harvest millions of people’s profiles. And built models to exploit what [Cambridge Analytica] knew about them and target their inner demons. That was the basis the entire company was built on.”¹

7. According to *The Washington Post*, Steve Bannon “oversaw Cambridge Analytica’s early efforts to collect troves of Facebook data as part of an ambitious program to build detailed profiles of millions of American voters[.]” “More than three years before he served as Trump’s chief political strategist, Bannon helped launch Cambridge Analytica with the financial backing of the wealthy Mercer family as part of a broader effort to create a populist power base.”²

8. Indeed, as noted by *The Inquirer*, President Donald Trump appeared to have

¹ Carole Cadwalladr and Emma Graham-Harrison, *Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach*, The Guardian (March 17, 2018), <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election>

² C. Timberg, K. Adam and M. Kranish, *Bannon oversaw Cambridge Analytica’s collection of Facebook data, according to former employee*, The Washington Post, (March 20, 2018), https://www.washingtonpost.com/politics/bannon-oversaw-cambridge-analyticas-collection-of-facebook-data-according-to-former-employee/2018/03/20/8fb369a6-2c55-11e8-b0b0-f706877db618_story.html?utm_term=.beb74a8561c4

acknowledged this scheme in a tweet at 5:44 AM on March 22, 2016³:

Donald J. Trump

@realDonaldTrump

Remember when they were saying, during the campaign, that Donald Trump is giving great speeches and drawing big crowds, but he is spending much less money and not using social media as well as Crooked Hillary's large and highly sophisticated staff. Well, not saying that anymore!

6:40 AM - Mar 22, 2018

92.7K 66.2K people are talking about this

9. Facebook claimed to have privacy policies and practices that protect the sensitive personal information that it collects, those policies and practices were woefully inadequate. Facebook promised that it would protect its members' information, consistent with industry standards and federal and state law. It did not. Having done Cambridge Analytica the favor of compiling the sensitive information of tens of millions of individuals in one place, Facebook failed to take steps to prevent its exploitation and improper access. Facebook has yet to come forth with a full and candid description of all facts known only to it concerning the unprecedented disclosure of millions of Facebook users' highly sensitive personal information, what Facebook has admitted is damning.

10. Facebook admits that it allowed third parties to access a vast amount of Facebook users' personal information. What is more troubling, by at least 2015, Facebook was aware that

³ Will Bunch, '*Race Realism': How Steve Bannon, Cambridge Anaylytica modernized white supremacy to elect Trump,* The Inquirer (March 22, 2018), http://www.philly.com/philly/columnists/will_bunch/race-realism-steve-bannon-cambridge-analytica-elected-trump-20180322.html.

information had been harvested on an unprecedented scale to be used by Cambridge Analytica to build a powerful software program to predict and influence the 2016 election. At the time, Facebook failed to alert users and failed to secure the private information of more than 50 million individuals.

11. Because Defendants' actions and omissions violate well established legal and statutory duties that they owed to Plaintiffs and all other similarly situated U.S. consumers, those individuals were forced to suffer the consequences.

12. Plaintiffs brings this class action on behalf of themselves and all similarly situated consumers for actual and statutory damages, as well as punitive damages and equitable relief to fully redress the vast harm Defendants' wrongful acts have unleashed on U.S. consumers.

JURISDICTION AND VENUE

13. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. §§ 1331 and 1337, as well as jurisdiction over the state law claims pursuant to 28 U.S.C. §§ 1332(d) and 1367 because this is a class action in which the matter or controversy exceeds the sum of \$5,000,000, exclusive of interest and costs, and in which some members of the proposed Classes are citizens of a state different from the Defendants.

14. Venue is proper in this District pursuant to 28 U.S.C. §§ 1391 (b), (c), and (d), because a substantial part of the events giving rise to Plaintiffs' claims occurred in this District.

15. This Court has personal jurisdiction because Defendants do business in this District and a substantial part of the events and injury giving rise to Plaintiffs' claims occurred in this District.

PARTIES

Plaintiffs

16. Plaintiff Jay Malskoff is a citizen of Edgewater, New Jersey and a registered

voter. Plaintiff has held a Facebook account for approximately 15 years. During the 2016 election cycle, Plaintiff was targeted with political advertisements while using Facebook.

17. Plaintiff Kenneth Irvine is a citizen of San Jose, California and a registered voter. Plaintiff has held a Facebook account for approximately 13 years. During the 2016 election cycle, Plaintiff was targeted with political advertisements while using Facebook

Defendants

18. Facebook is a Delaware corporation that operates an online social media and social networking service that allows people to communicate with their family, friends, and coworkers. Its website was launched on February 4, 2004, by Mark Zuckerberg, along with fellow Harvard College students and roommates, Eduardo Saverin, Andrew McCollum, Dustin Moskovitz, and Chris Hughes. Facebook's principal place of business is located in Menlo Park, California. Facebook's securities trade on the NASDAQ under the ticker symbol "FB."

19. Cambridge Analytica is a political consulting firm which offers data mining, analysis, and behavioral communication solutions for the electoral process. By its own description, Cambridge Analytica engages in the business of "behavioral microtargeting" – the collating and/or creating and then selling data profiles of individuals which are used for targeted advertisements and political campaigning. It was formed by its British parent company SCL Group Limited, which offers similar services around the world.

20. Cambridge Analytica CEO Alexander Nix has said Cambridge Analytica was involved in 44 U.S. political races in 2014. In 2015, it performed data analysis services for Senator Ted Cruz's presidential campaign. In 2016, Cambridge Analytica worked for Donald Trump's presidential campaign and on the Leave.EU campaign for the United Kingdom's withdrawal from the European Union (commonly referred to as "Brexit"). Cambridge Analytica's role in those campaigns is the subject of ongoing criminal investigations in both

countries.

21. CA UK1 and CA UK2 are British-registered companies headquartered in London, England with U.S. offices located in New York, New York and Washington D.C. Prior to changing its name, CA UK1 was formerly registered as SCL USA LIMITED.

22. CA USA is a Delaware limited liability company with its principal place of business located in New York, New York.

23. Mercer is an individual resident of New York, New York. Mercer, an American hedge-fund manager known for his far-right conservative positions, reportedly invested millions of dollars in Cambridge Analytica, and Rebekah Mercer (Mercer's daughter) sits on Cambridge Analytica's Board of Directors. *The Guardian* reported that Mercer met with Cambridge Analytica's CEO Alexander Nix and Christopher Wylie in New York, New York to discuss the plan to harvest and use Facebook users' data in order to create sophisticated psychological and political profiles. Wylie told *The Guardian* about that meeting, stating Mercer "said very little, but he really listened. He wanted to understand the science. And he wanted proof that it worked."⁴

24. Kogan is an individual resident of Cambridge, England. Kogan contracted to work with Cambridge Analytica and designed the plan to acquire user data. According to the report:

...he advertised for people who were willing to be paid to take a personality quiz on Amazon's Mechanical Turk and Qualtrics. At the end of which Kogan's app, called thisismydigitallife, gave him permission to access their Facebook profiles. And not just theirs, but their friends' too. On average, each 'seeder' – the people who

⁴ Carole Cadwalladr, *The Cambridge Analytica Files 'I made Steve Bannon's psychological warfare tool': meet the data war whistleblower*, The Guardian (March 18, 2018), <https://www.theguardian.com/news/2018/mar/17/data-war-whistleblower-christopher-wylie-facebook-nix-bannon-trump>

had taken the personality test, around 320,000 in total – unwittingly gave access to at least 160 other people’s profiles, none of whom would have known or had reason to suspect.

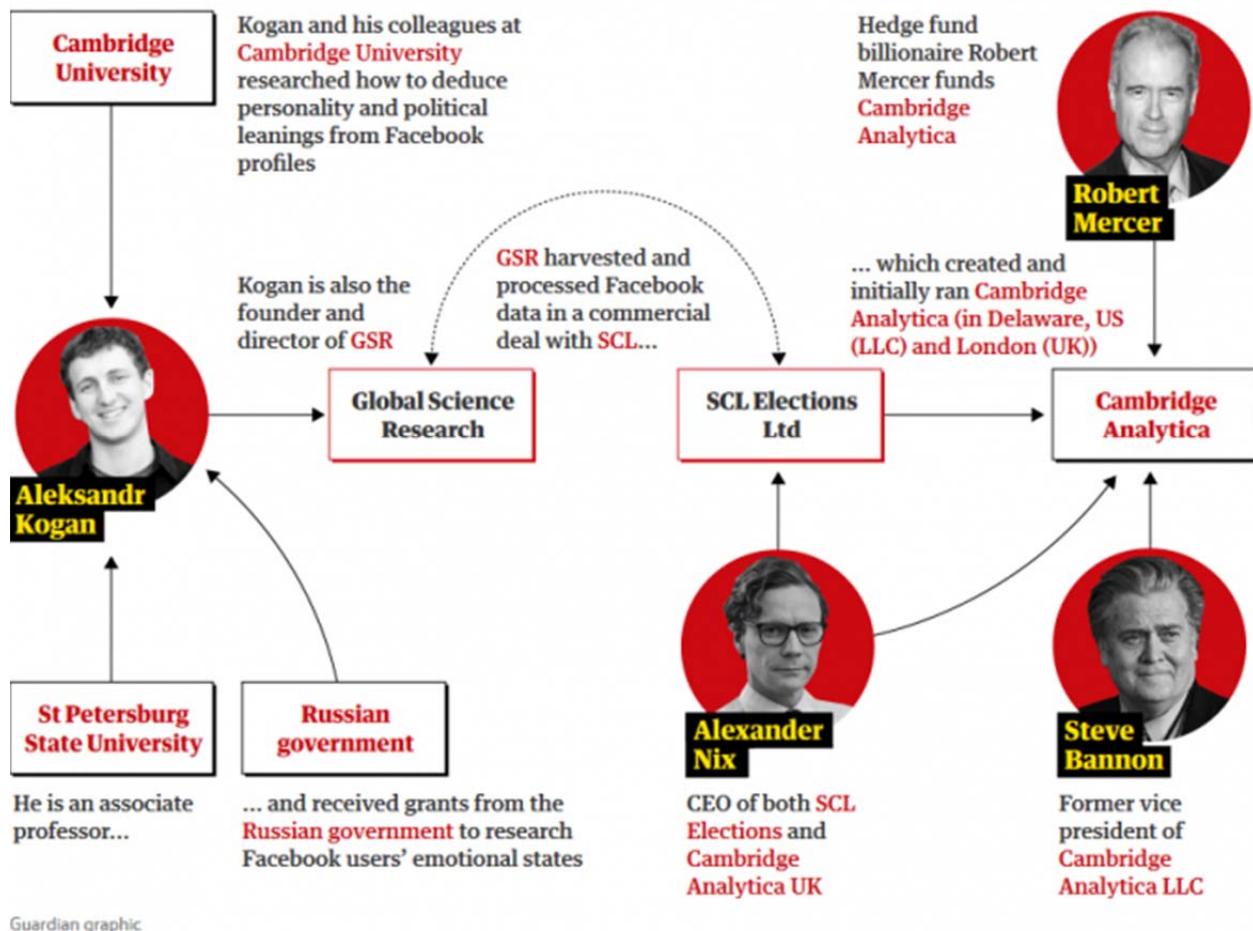
This scheme allowed Kogan to collect “millions of profiles in a matter of weeks.” Kogan did all of this in the employ of Cambridge Analytica, to help aggregate a massive dataset that would allow Cambridge Analytica to target users for the purpose of influencing their political preferences through advertising and misinformation.⁵

25. While Cambridge Analytica has not disclosed an organizational chart, *The Guardian* created the following graphic depicting the key players⁶:

⁵ *Id.*

⁶ Carole Cadwalladr and Emma Graham-Harrison, *Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach*, The Guardian (March 17, 2018), <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election>

Cambridge Analytica: how the key players are linked



Guardian graphic

26. Defendants do business nationwide, including in this District.

FACTUAL ALLEGATIONS

27. Facebook develops technologies that facilitate the sharing of information, photographs, website links, and videos. By the end of 2017, Facebook had more than 2.2 billion active users. Facebook's purported mission is "to give people the power to build community and bring the world closer together. People use Facebook to stay connected with friends and family, to discover what's going on in the world, and to share and express what matters to them."

28. While Facebook may have started as a social network, Facebook's business model has shifted into what is now one of the largest data mining companies in the world—designed to

harness and sell the ability to influence its users' behavior.⁷ And, by providing companies with all the tools needed to influence and manipulate its users, Facebook generates billions of dollars in revenue each year. Indeed, Facebook reported \$12.7 billion in revenue for the fourth quarter 2017 alone, with profits of \$4.26 billion – once again demonstrating the company's dominance in social media advertising. The social platform will capture 18.4% of the \$266 billion global digital advertising market in 2018.

29. As a purported social media leader, Facebook knows the critical importance of protecting users' personal information from unauthorized access. Facebook also knows the multitude of harms that foreseeably flow to individual users when information is stolen or misused by criminals. Facebook's "Data Use Policy" emphasizes "trust" and states that "we don't share information we receive about you with others unless we have ... received your permission [and] given you notice."

30. In contrast to Facebook's policies, during the 2016 Presidential election, while using Facebook to connect with friends and family, Plaintiffs and Class members were targeted with political advertisements and posts specifically tailored for them based on information mined from their Facebook profiles. Although Facebook has now (under pressure from its users and three years too late) condemned Cambridge Analytica's unauthorized harvesting of users' data, Cambridge Analytica's actions are consistent with Facebook's true mission—to use its users' information to drive revenue.

31. Wylie revealed how the data mining worked on Facebook's platform: "With their profiles, likes, even private messages, [Cambridge Analytica] could build a personality profile on

⁷ Sam Machkovech, *Report: Facebook helped advertisers target teens who feel "worthless"* [Updated], ArsTechnica (May 1, 2007), <https://arstechnica.com/information-technology/2017/05/facebook-helped-advertisers-target-teens-who-feel-worthless>

each person and know how best to target them with messages.”⁸

32. Wylie stated that he had receipts, invoices, emails, legal letters and records that “showed how, between June and August 2014, the profiles of more than 50 million Facebook users had been harvested.”⁹ These profiles “contained enough information, including places of residence, that [Cambridge Analytica] could match users to other records and build psychographic profiles.”¹⁰

33. Cambridge Analytica then mounted a campaign of psychological warfare on millions of Facebook users, without their knowledge or consent. Of the 50 million Facebook users victimized by this scheme, “only about 270,000 users – those who had participated in the [my digital life] survey” – had even consented to having any of their data harvested, and then only for research purposes, and without any authorization to having their data used to promote Cambridge Analytica’s and Mercer’s political goal to engage in cultural warfare. Indeed, Wylie stated that “the Facebook data...was ‘the saving grace’ that let his team deliver the models it had promised the Mercers.”¹¹

A. FACEBOOK PERMITTED KOGAN AND CAMBRIGE ANALYTICA TO HARVEST AND USE FACEBOOK USERS’ PERSONAL INFORMATION FOR POLITICAL GAIN

34. Between 2010 and 2015, Facebook allowed third-party apps to collect extensive personal data from users and their friends. Indeed, because it receives significant monetary gain

⁸ Parmy Olson, *Face-To-Face-with-Cambridge Analytica’s Alexander Nix*, Forbes (March 20, 2018), <https://www.forbes.com/sites/parmyolson/2018/03/20/face-to-face-with-cambridge-analytica-alexander-nix-facebook-trump/#51eb9142535f>

⁹ Carole Cadwalladr, *The Cambridge Analytica Files ‘I made Steve Bannon’s psychological warfare tool’: meet the data war whistleblower*, The Guardian (March 18, 2018), <https://www.theguardian.com/news/2018/mar/17/data-war-whistleblower-christopher-wylie-facebook-nix-bannon-trump>

¹⁰ M. Rosenberg, N. Confessore and C. Cadwalladr, *How Trump Consultants Exploited the Facebook Data of Millions*, New York Times (March 17, 2018), <https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html>

¹¹ *Id.*

by permitting targeted advertising and is uniquely positioned to accumulate specific consumers' online and offline behaviors, Facebook encouraged third party developers to utilize its platform to collect users' personal information.

35. In 2010, Facebook launched Open Graph API version 1.0 for developers, which allowed extensive user data collection, including users' friends' information, without having to communicate the reasoning for acquiring such data.

36. These apps could acquire a comprehensive dataset that included a user's public profile (their name, gender, location, time zone, and Facebook ID), as well as their friends' names, bios, birthdays, education, political views, relationship status, religion, notes, chat online status, and more. With extended permissions, developers could even gain access to a user's private messages.

37. That same year, Facebook CEO Mark Zuckerberg wrote a *Washington Post* op-ed vowing to redesign the site's privacy policy in order to offer more granular control of data permissions and to reduce the amount of user information available to the public.¹²

38. In 2012, however, in contrast to his public statements, Facebook tweaked the design of its permissions request page to make it less apparent to users that they were handing over more personal information.

39. Screenshots from 2012 show how Facebook changed the options on the permissions page for games from "Allow" and "Don't Allow" to simply "Play Game," the latter of which did not communicate clearly to users that they were opting into sharing data. The new design also hid its explanation of what it considered "basic information" underneath a small "?"

¹² Mark Zuckerberg, *From Facebook, answering privacy concerns with new settings*, Washington Post (May 24, 2010), <http://www.washingtonpost.com/wp-dyn/content/article/2010/05/23/AR2010052303828.html>

symbol that users needed to hover over to read.¹³

40. According to *Techcrunch.com*, “Facebook keeps ‘improving’ their design so that more of us will add apps on Facebook without realizing we’re granting those apps (and their creators) access to our personal information. After all, this access to our information and identity is the currency Facebook is trading in and what is driving its stock up or down.”¹⁴

41. In 2013, under the guise of performing research, Cambridge University researcher Aleksandr Kogan developed a quiz app using Graph API. Over 270,000 users took the survey, giving away their own data, plus friends’ data. More specifically, using a firm called “Global Science Research,” Kogan hired people to take his personality quiz on Amazon Mechanical Turk, a site that connects workers with jobs that require simple tasks for a fee. According to *The Intercept*, Kogan paid \$1 or \$2 to workers to complete the survey using their Facebook accounts.¹⁵

42. By requiring the use of Facebook to complete the “research” survey and because of the way Facebook’s third-party platform worked at the time, the over 270,000 survey participants who consented to hand over their data also gave Kogan (and Cambridge Analytica) access to tens of millions of their friends’ Facebook data. Kogan told Facebook and its users that the data would be anonymized, but it wasn’t.

43. In now-deleted tweets, Facebook executive Alex Stamos said that while Kogan did not break into any systems “[h]e did … misuse that data after he gathered it[.]” Stamos’

¹³ *5 Design Tricks Facebook Uses to Affect Your Privacy Decisions*, TechCrunch (Aug. 25, 2010), <https://techcrunch.com/2012/08/25/5-design-tricks-facebook-uses-to-affect-your-privacy-decisions/>

¹⁴ *Id.*

¹⁵ Matthias Schwartz, *Facebook Failed to Protect 30 Million Users From Having Their Data Harvested by Trump Campaign Affiliate*, The Intercept (March 30, 2017), <https://theintercept.com/2017/03/30/facebook-failed-to-protect-30-million-users-from-having-their-data-harvested-by-trump-campaign-affiliate/>

now-deleted tweets describe how Kogan and Cambridge Analytica used the app to harvest millions of Facebook users' data:

The recent Cambridge Analytica stories by the NY Times and The Guardian are important and powerful, but it is incorrect to call this a "breach" under any reasonable definition of the term. We can condemn this behavior while being accurate in our description of it.

At the time of this quiz, the Facebook API allowed app developers to see a larger portion of the data available to a user than we do now. This included names and likes from friends. There were privacy controls available to both the user of the app and their friends.

The ability to get friend data via API, with the permission of a user, was documented in our terms of service, platform documentation, the privacy settings, and the screen used to login to apps.

In 2015, we updated our APIs to remove the ability to see this kind of friend data. This was controversial with app developers at the time, but was the right decision to increase privacy and reduce the chance of abuses like this.

It should be noted that several other prominent platforms, like Android and iOS, allow access to friend (contact) data with user permission. Like us, those platforms have policies about the use of data, but mining contacts gathered knowingly from a phone is also not a "breach".

I am not defending Kogan or Cambridge Analytica, but we can have a discussion of their inappropriate actions while also accurately describing them.

11:35 AM - 17 Mar 2018

44. Facebook has an all-embracing history of harvesting its users' personal information under the guise of research. For example, in 2014, Facebook published a study about a News Feed experiment to influence users' emotions. The study's publication prompted widespread outrage over privacy concerns on Facebook. Facebook users were furious at Facebook for having performed the research without more explicit consent.¹⁶

45. In the study, Facebook subjected nearly 700,000 users to a 2012 study in an attempt to discover how to make people feel happier or sadder, based on what Facebook showed them on their News Feed. They found that users who saw more negative posts tended to write more negative posts themselves, and vice versa.¹⁷

¹⁶ *We all really are just rats in the Facebook maze*, MetaFilter Community WebBlog (June 28, 2014), <https://www.metafilter.com/140307/We-all-really-are-just-rats-in-the-Facebook-maze>

¹⁷ Adam D. I. Kramer, *Experimental evidence of massive-scale emotional contagion through*

46. Facebook said in its study that it followed its own data use policy, which states that all users agree, before creating an account, to informed consent for this research. However, *Forbes* reported that the “research policy” clause in the site’s terms was added in May 2012, four months after the study took place.¹⁸

47. Facebook routinely conducted, and still conducts, experiments using its users’ personal information for reasons including prompting users to click more links, or more ads, which are the company’s main source of revenue. Indeed, Facebook has an entire Data Science team whose sole aim is to harvest Facebook’s user data and has “conducted studies on everything from who is attending the World Cup to how users’ communications change after partners break up with them and whether upbeat messages spread more quickly than negative ones.”¹⁹

48. The purpose of such research was to demonstrate Facebook’s influence over user behavior and the power its platform has to manipulate emotions. For this reason, by carrying out its research, Facebook invited companies like Cambridge Analytica to harvest users’ personal information and use it to tailor messages that would influence and manipulate their behavior.

49. In 2015, Facebook shut down access to its Graph API and updated its platform to give away less data, especially about users’ friends. Facebook also offered more granular control over what information its users shared with developers, and a new login screen with an added “Edit the info you provide” link. However, permissions for Facebook apps enabled between

social networks, PNAS (June 17, 2014), <http://www.pnas.org/content/111/24/8788>

¹⁸ Kashmir Hill, *Facebook Added ‘Research’ To User Agreement After Emotion Manipulation Study*, *Forbes* (June 30, 2014), <https://www.forbes.com/sites/kashmirhill/2014/06/30/facebook-only-got-permission-to-do-research-on-users-after-emotion-manipulation-study/#163346e7a62d>

¹⁹ Reed Albergotti and Elizabeth Dwoskin, *Facebook Study Sparks Soul-Searching and Ethical Questions*, *The Wall Street Journal* (June 30, 2014), <https://www.wsj.com/articles/facebook-study-sparks-ethical-questions-1404172292>

2010 and 2015 were not retroactively limited, and it is highly likely third parties stored data collected from Facebook users on their own servers.

50. That same year, through an inquiry from *The Guardian*, Facebook learned that Kogan had sold the Facebook user dataset he acquired for “research purposes” to Cambridge Analytica.

51. Facebook verified that the firm had acquired user data, but did not publicly acknowledge it. According to Facebook, Cambridge Analytica “certified in a legal document that they had deleted the data,” which Facebook explained is the reason why it never suspended Kogan, Global Science Research, or Cambridge Analytica from its platform at the time.²⁰

52. Facebook, however, did not undertake any reasonable measures to ensure that Cambridge Analytica deleted the personal information of Facebook users that was unlawfully obtained by Cambridge Analytica. Facebook has now conceded that Cambridge Analytica did not delete the sensitive personal information of millions of Facebook users. According to CEO Mark Zuckerberg’s March 21, 2018 Facebook post:

Last week, we learned from The Guardian, The New York Times and Channel 4 that Cambridge Analytica may not have deleted the data as they had certified. We immediately banned them from using any of our services. Cambridge Analytica claims they have already deleted the data and has agreed to a forensic audit by a firm we hired to confirm this. We’re also working with regulators as they investigate what happened.²¹

53. Indeed, Wylie told *The Guardian*, “Facebook made zero effort to get the data back. There were multiple copies of it. It had been emailed in unencrypted files.”²²

²⁰ Boz, Facebook Post (March 19, 2018 at 3:56pm), <https://www.facebook.com/boz/posts/10104702799873151?pnref=story>

²¹ Mark Zuckerberg, Facebook Post (March 21, 2018 at 3:36pm, Menlo Park, CA), <https://www.facebook.com/zuck/posts/10104712037900071>

²² Carole Cadwalladr, *The Cambridge Analytica Files ‘I made Steve Bannon’s psychological*

54. In 2016, then-presidential candidate Donald Trump's campaign hired Cambridge Analytica. Donald Trump's campaign began investing heavily in Facebook advertising ahead of the presidential election. A super PAC supporting Donald Trump directed an anti-Hillary Clinton video advertisement aimed at specific audience segments identified by Cambridge Analytica. An investigation by Channel 4 in England showed Mark Turnbull, a managing director of Cambridge Analytica, claiming the firm was responsible for the "Defeat Crooked Hillary" video campaign on Facebook.²³

55. Cambridge Analytica claims to have "provided the Donald J. Trump for President campaign with the expertise and insight that helped win the White House"²⁴ by supplying the campaign with its psychographic profiling of millions of Facebook users – all enabled by Facebook.

56. On March 17, 2018, *The New York Times* and *The Guardian* reported that Cambridge Analytica still possesses data it inappropriately gathered from as many as 50 million Facebook users. Only after the reports were published, Facebook suspended Cambridge Analytica (and Wylie, the very whistleblower who revealed the fraudulent scheme to the public).²⁵

warfare tool': meet the data war whistleblower, The Guardian (March 18, 2018), <https://www.theguardian.com/news/2018/mar/17/data-war-whistleblower-christopher-wylie-facebook-nix-bannon-trump>

²³ *Exposed: Undercover secrets of Trump's data firm*, Channel 4 News (March 20, 2018), <https://www.channel4.com/news/exposed-undercover-secrets-of-donald-trump-data-firm-cambridge-analytica>

²⁴ Cambridge Analytica, Press Release, available at <https://political.com/casestudies/casestudydonaldjtrumpforpresident2016> (last visited March 27, 2018)

²⁵ Carole Cadwalladr and Emma Graham-Harrison, *Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach*, The Guardian (March 17, 2018), <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election>; M. Rosenberg, N. Confessore and Carole Cadwalladr, *How Trump Consultants Exploited the Facebook Data of Millions*, New York Times (March 17, 2018),

57. On March 21, 2018, Facebook CEO Zuckerberg broke his silence and announced a new tool that offers an easy way to revoke apps' permissions to access users' data. He also acknowledged that Facebook had breached its users' trust and was irresponsible with users' sensitive personal information:

We have a responsibility to protect your data, and if we can't then we don't deserve to serve you.... This was a breach of trust between Kogan, Cambridge Analytica and Facebook. But it was also a breach of trust between Facebook and the people who share their data with us and expect us to protect it. We need to fix that.²⁶

58. In addition, CEO Zuckerberg announced that Facebook would no longer allow app developers access to its users' data after three months of inactivity, that it would reduce the information people are required to give app developers, and that it would audit all apps with access to large amounts of data. Yet, despite its knowledge of Cambridge Analytica's misuse of users' personal information years ago, and until the news story broke, Facebook had not undertaken reasonable measures to "prevent bad actors from accessing people's information in this way."²⁷

59. CEO Zuckerberg's March 21, 2018 Facebook post also failed to explain why neither he nor Facebook took any action to notify Facebook users in 2013, 2014, 2015, 2016, or 2017 that Kogan or Cambridge Analytica had "misused personally identifiable information."²⁸

B. FACEBOOK KNEW ITS PRIVACY SETTINGS WERE FLAWED AND PERMITTED UNAUTHORIZED HARVESTING OF USERS' PERSONAL INFORMATION

60. Even before it learned of Cambridge Analytica's mining and misuse of its users'

<https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html#click=https://t.co/UAq1Q5t1BG>

²⁶ Mark Zuckerberg, Facebook Post (March 21, 2018 at 3:36pm, Menlo Park, CA), <https://www.facebook.com/zuck/posts/10104712037900071>

²⁷ *Id.*

²⁸ *Id.*

data in 2015, Facebook was well-aware of the dangers of its lax approach to users' personal information. Facebook, however, overlooked its vulnerabilities because it was good for business—especially as it looked to maximize and diversify its revenue streams

61. Sandy Parakilas, a former “platforms operations manager at Facebook responsible for policing data breaches by third party software developers between 2011 and 2012,” stated that as many as hundreds of millions of Facebook users are likely to have had their private information harvested by companies that exploited the same terms as the firm that collected data and passed it on to Cambridge Analytica.”²⁹

62. Parakilas warned senior executives at Facebook that its lax approach to data protection risked a major breach: “[Parakila’s] concerns were that all of the data that left Facebook servers to developers could not be monitored by Facebook, so [Facebook] had no idea what developers were doing with the data” and that Facebook did not use enforcement mechanisms, including audits of external developers, to ensure data was not being misused.³⁰

63. Parakilas stated that “[Facebook] felt that it was better not to know.”³¹ Despite Parakilas’ warnings, Facebook’s lax approach to data protection remained – as evinced by Cambridge Analytica’s harvesting and misuse of Facebook users’ personal information.

64. The Federal Trade Commission (“FTC”) also warned Facebook and mandated change to Facebook’s privacy settings – which again went ignored. On March 20, 2018, the FTC launched an inquiry into Facebook and Cambridge Analytica. The FTC is investigating whether Facebook violated a settlement reached with the government agency in 2011 over user

²⁹ Paul Lewis, ‘Utterly horrifying’: ex-Facebook insider says covert data harvesting was routine, The Guardian (March 20, 2018), <https://www.theguardian.com/news/2018/mar/20/facebook-data-cambridge-analytica-sandy-parakilas>

³⁰ *Id.*

³¹ *Id.*

privacy protections. The FTC back in 2011 had explicitly punished Facebook for allowing users' personal data to be shared when their friends signed up for an app — the same process Kogan and Cambridge used to grow its data pool from 270,000 quiz app users to their tens of millions of friends.

65. The FTC said at the time that "Facebook told users they could restrict sharing of data to limited audiences — for example with 'Friends Only.' In fact, selecting 'Friends Only' did not prevent their information from being shared with third-party applications their friends used." The FTC found that Facebook falsely represented that third-party apps that users installed would have access only to user information that they needed to operate because the apps could access nearly all of users' personal data — "data the apps didn't need."³²

66. Under the 2011 settlement with the FTC, Facebook "agreed to get user consent for certain changes to privacy settings as part of a settlement of federal charges that it deceived consumers and forced them to share more Personal Information than they intended." *Bloomberg* reported that "if the FTC finds Facebook violated terms of the consent decree, it has the power to fine the company more than \$40,000 a day per violation."³³

67. Had Facebook implemented the necessary and required privacy reforms, the misconduct committed by Kogan and Cambridge Analytica may not have occurred.

68. As a direct and proximate result of Defendants' actions and omissions, Plaintiffs and similarly situated consumers have been harmed, injured, and damaged. Plaintiffs and members of the Classes have been injured through unauthorized harvesting and use of their

³² FTC, *Facebook Settles FTC Charges That It Deceived Consumers By Failing To Keep Privacy Promises* (November 29, 2011), <https://www.ftc.gov/news-events/press-releases/2011/11/facebook-settles-ftc-charges-it-deceived-consumers-failing-keep>

³³ Bloomberg, *FTC probing Facebook for use of personal data*, The OCR (March 20, 2018), <https://www.ocregister.com/2018/03/20/ftc-probing-facebook-for-use-of-personal-data>

personal information, as well as the multitude of harms that are likely to follow from such access and use.

CLASS ALLEGATIONS

69. Plaintiffs bring all claims as class claims under Rules 23(b)(2), (b)(3), and (c)(4) of the Federal Rules of Civil Procedure.

70. Plaintiffs bring their claims on behalf of a proposed nationwide class (“**National Class**”), defined as follows:

All persons who registered for Facebook accounts in the United States and whose personal information was obtained from Facebook by Cambridge Analytica without authorization or in excess of authorization.

71. Plaintiff Jay Malskoff also brings his claims under New Jersey consumer and data protection statutes on behalf of a proposed statewide subclass (“**New Jersey Subclass**”), defined as follows:

All New Jersey residents who registered for Facebook accounts in the United States and whose personal information was obtained from Facebook by Cambridge Analytica without authorization or in excess of authorization.

72. Plaintiff Kenneth Irvine also brings his claims under California consumer and data protection statutes on behalf of a proposed statewide subclass (“**California Subclass**”), defined as follows:

All California residents who registered for Facebook accounts in the United States and whose personal information was obtained from Facebook by Cambridge Analytica without authorization or in excess of authorization.

73. The National Class, the New Jersey Subclass, and the California Subclass are referred to, collectively, as the Classes.

74. Excluded from the Classes are: the Defendants; any of their corporate affiliates;

any of their directors, officers, or employees; any persons who timely elects to be excluded from any of the Classes; any government entities; and any judge to whom this case is assigned and their immediate family and court staff.

75. Plaintiffs do not know the exact number of members in the Classes, but believe that there are millions of members. The members of the Classes are so numerous that joinder of all members of any Class would be impracticable. The names and addresses of Class members are identifiable through documents maintained by Defendants.

76. Common questions of law and fact exist as to all members of the Classes and, as appropriate, the members of each Subclass. The data breach was generally applicable to all the members of the Classes and arose from a common set of acts and omissions by Defendants without regard to the nature or identity of individual class members, thereby making appropriate relief with respect to the Classes as a whole.

77. The questions of law and fact common to the Classes include:

- (a) Whether Facebook represented that it would safeguard Plaintiff's and Class members' personal information and not disclose it without consent;
- (b) Whether Facebook owed a duty to the Class members under federal or state law to protect their personal information, provide timely notice of the unauthorized access, provide timely and accurate information as to the extent of the compromised personal information, and provide meaningful and fair redress;
- (c) Whether Facebook breached such duty;
- (d) Whether Facebook's breach provided the means for the data breach;
- (e) Whether Facebook was negligent in failing to design, employment, and maintain adequate privacy systems and protocols;

- (f) Whether Facebook's negligence provided the means for the data breach;
- (g) Whether Facebook knew or reasonably should have known of the vulnerabilities in its systems that allowed for the unauthorized access;
- (h) Whether Facebook willfully failed to design, employ, and maintain a system adequate to protect the personal information at issue;
- (i) Whether representations Facebook made about its systems security were false or misleading;
- (j) Whether Cambridge Analytica improperly obtained Plaintiffs' and Class members' personal information without authorization or in excess of any authorization;
- (k) Whether Facebook was aware of Cambridge Analytica's improper collection of Plaintiffs' and Class members' personal information;
- (l) Whether Defendants' actions and omissions violated applicable state consumer protection laws;
- (m) Whether Defendants' conduct violated the Stored Communications Act, 18 U.S.C. §§ 2701, *et seq.*;
- (n) Whether Defendants' engaged in a civil conspiracy to violate the Stored Communications Act, 18 U.S.C. §§ 2701, *et seq.*;
- (o) Whether Defendants' actions and omissions were the proximate cause of the data breach and the resulting injuries to Plaintiffs and the Classes;
- (p) Whether Plaintiffs and the Classes were injured as a result of the unauthorized access and use of their personal information;

- (q) Whether injuries to Plaintiffs and the Classes were exacerbated by Facebook's failure to provide timely and accurate notice of the breach and impact on their personal information; and
- (r) The appropriate injunctive and related equitable relief for the Classes; and
- (s) The appropriate class-wide measure of damages for the Classes.

78. Plaintiffs' claims are typical of the claims of the members of the Classes (and their respective Subclasses), and Plaintiffs will fairly and adequately protect the interests of the Classes. Plaintiffs and all members of the Classes are similarly affected by Defendants' wrongful conduct in that their personal information has been exposed and used without their authorization or in excess of any authorization.

79. Plaintiffs' claims arise out of the same common course of conduct giving rise to the claims of the other members of the Classes.

80. Plaintiffs' interests are coincident with, and not antagonistic to, those of the other members of the Classes.

81. Plaintiffs are represented by counsel competent and experienced in the prosecution of consumer protection and tort litigation.

82. The questions of law and fact common to the members of the Classes predominate over any questions affecting only individual members, including legal and factual issues relating to liability and damages.

83. Class action treatment is a superior method for the fair and efficient adjudication of the controversy. Among other things, such treatment will permit a large number of similarly situated persons to prosecute their common claims in a single forum simultaneously, efficiently and without the unnecessary duplication of evidence, effort and expense if numerous individual

actions. The benefits of proceeding as a class, including providing injured persons with a method for obtaining redress for claims that might not be practicable to pursue individually, substantially outweigh any potential difficulties in managing this class action.

84. The prosecution of separate actions by individual members of the Classes is not feasible and would create a risk of inconsistent or varying adjudications.

FIRST COUNT

**Violation of the Stored Communications Act
18 U.S.C. §§ 2701, *et seq.***

85. Plaintiffs incorporate by reference the allegations in the preceding paragraphs as if fully set forth herein.

86. Under the Stored Communications Act (“SCA”), an entity providing an electronic communication service to the public “shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service.” 18 U.S.C. § 2702(a)(1).

87. The SCA allows a private right of action against anyone who “(1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or (2) intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system.” *See* 18 U.S.C. § 2701(a); *see also id.* § 2707(a) (cause of action).

88. The court may assess damages under the SCA including “actual damages suffered by the plaintiff and any profits made by the violator as a result of the violation, but in no case shall a person entitled to recover receive less than the sum of \$1,000.” 18 U.S.C. § 2707(c).

89. Facebook and Cambridge Analytica are electronic communications providers within the meaning of the SCA.

90. Facebook and Cambridge Analytica intentionally exceeded any authorization they may have had to Plaintiffs' and Class members' stored electronic communications by allowing Cambridge Analytica to have access to Plaintiffs' and Class members' stored electronic communications which also contained sensitive personal information.

91. Facebook and Cambridge Analytica knowingly allowed Cambridge Analytica and as yet unknown third parties to intentionally exceed any authorization it may have had to Plaintiffs' and Class members' stored electronic communications.

92. Kogan and Mercer are persons under the SCA also liable for any violations of the Act.

93. Further, Kogan and Mercer knew of Cambridge Analytica's unlawful scheme and provided aid and assistance to Cambridge Analytica's unauthorized access and collection of user data.

94. As a result of Defendants' actions, Plaintiffs and the Class members are entitled to statutory damages, actual damages, and reasonable attorney's fees and costs, as well as declaratory and injunctive relief.

SECOND COUNT

Negligence (against Facebook and Cambridge Analytica)

95. Plaintiffs incorporate by reference the allegations in the preceding paragraphs as if fully set forth herein.

96. Facebook owed Plaintiffs and the Class members a duty of care commensurate with the sensitive nature of the personal information with which it was entrusted (particularly when aggregated and digitized). Facebook created this duty through its voluntary actions in collecting and storing the personal information for its own benefit, as well as by its assurances

(in its Privacy Policy and elsewhere) that it would safeguard that information. In addition, given the nature of the information at issue and the means by which Facebook acquires it, the relationship between Plaintiffs and the Class members and Facebook is sufficiently close and akin to privity to give rise to a duty to the consumers.

97. Facebook's duty required it, among other things, to design and employ privacy systems and intrusion detection and reporting systems sufficient to protect personal information from being compromised, lost, stolen, misused, and disclosed to unauthorized parties, and to promptly alert Plaintiffs and Class members of any such access.

98. Facebook knew that the personal information of Plaintiffs and Class members was personal and sensitive information that is valuable.

99. Had Facebook designed, employed, and maintained appropriate technological and other systems, the personal information would not have been compromised or, at a minimum, Facebook would have known of the extent of the unauthorized access sooner and would be able to accurately inform Plaintiffs and the other Class members of the extent to which their personal information had been compromised.

100. By being entrusted by Plaintiffs and the Class members to safeguard their personal information, Facebook had a special relationship with Plaintiffs and the Class. Plaintiff and Class members signed up for Facebook's services and agreed to provide their personal information with the understanding that Facebook would take appropriate measures to protect it and would inform Plaintiffs and Class members of any breaches or other security concerns that might call for action by Plaintiffs and Class members.

101. Facebook breached its duties of care by, among other things, failing to maintain appropriate technological and other systems to prevent unauthorized access and to minimize the

personal information that any intrusion could compromise. Facebook also breached their duty to timely disclose that Plaintiffs' and Class members' personal information had been, or was reasonably believed to have been, improperly obtained.

102. Cambridge Analytica had a duty to refrain from obtaining Plaintiffs' and the Class members' personal information in without their consent or authorization or in excess of any authorization.

103. Cambridge Analytica breached its duty, and Facebook failed to prevent Cambridge Analytica's improper obtaining of Plaintiffs' and the Class members' personal information.

104. Defendants' breach of their duties provided the means for Plaintiffs' and Class members' personal information to be obtained and used without authorization. But for Defendants' wrongful and negligent breach of their duties owed to Plaintiffs and the Classes, their personal information would not have been improperly obtained.

105. The injury and harm suffered by Plaintiffs and the Class members was the reasonably foreseeable result of Defendants' failure to exercise reasonable care in safeguarding and protecting Plaintiffs' and the other Class members' personal information.

106. Plaintiffs and the members of the Classes are entitled to damages in an amount to be proven at trial.

THIRD COUNT

Unjust Enrichment/Quasi Contract (against Facebook and Cambridge Analytica)

107. Plaintiffs incorporate by reference all the above allegations as if fully set forth herein.

108. Defendants received millions of dollars in revenue from the sale and use of

Plaintiffs' and Class members' personal information. Cambridge Analytica's psychographic mapping tool was crucial to President Trump's campaign strategy and its success. President Trump won the election, and Cambridge Analytica earned millions of dollars and confirmed its ability to manipulate voters' behavior.

109. These millions in revenue was a benefit conferred upon Defendants by Plaintiffs and the Classes.

110. Defendants were unjustly enriched through financial benefits conferred upon it by Plaintiffs and the Classes.

111. Therefore, because Defendants will be unjustly enriched if it is allowed to retain the revenues obtained through falsehoods, deception and breach of trust, Plaintiffs and each Class Member are entitled to recover the amount by which Defendants were unjustly enriched at his or her expense.

112. Accordingly, Plaintiffs, on behalf of themselves and each Class member, seek damages against Defendants in the amounts by which Defendants have been unjustly enriched at Plaintiffs' and each Class Member's expense, and such other relief as this Court deems just and proper

FOURTH COUNT

Civil Conspiracy (against Kogan, Cambridge Analytica, and Mercer)

113. Plaintiffs incorporate by reference all the above allegations as if fully set forth herein.

114. A civil conspiracy is composed of two or more persons combining to accomplish an unlawful purpose or to accomplish a lawful purpose by unlawful means. The elements of a cause of action for civil conspiracy are (1) two or more persons; (2) an object to be

accomplished; (3) a meeting of the minds on the object or course of action; (4) one or more unlawful, overt acts; and (5) damages as the proximate result.

115. Kogan, Cambridge Analytica, and Mercer conspired to harvest Facebook users' data without authorization or in excess of any authorization. Defendants' entire business relationship was premised on this act, which violated users' privacy rights codified by the SCA.

116. Defendants' conspired to harm Plaintiffs and Class members by secretly and unlawfully harvesting data without users' or Facebook's consent.

117. Kogan was able to obtain user data without authorization or in excess of any authorization because Cambridge Analytica and Mercer funded the advertising and labor necessary to achieve their unlawful purpose.

118. As a result of Defendants' conspiracy, Plaintiffs and the Class are entitled to compensatory and statutory damages and injunctive relief from Kogan, Cambridge Analytica, and Mercer for their participation in violating Plaintiffs' and Class members' privacy rights.

FIFTH COUNT

Violation of New Jersey Consumer Fraud Act N.J. STAT. ANN. § 56:8-1, *et seq.* (against Facebook and Cambridge Analytica)

119. Plaintiffs incorporate by reference the allegations in the preceding paragraphs as if fully set forth herein.

120. Defendants and the New Jersey State Class members are "persons" within the meaning of N.J. STAT. ANN. § 56:8-1(d). Facebook and Cambridge Analytica engaged in "sales" of "merchandise" within the meaning of N.J. STAT. ANN. § 56:8-1(c), (d).

121. The New Jersey Consumer Fraud Act ("New Jersey CFA") makes unlawful "[t]he act, use or employment by any person of any unconscionable commercial practice, deception, fraud, false pretense, false promise, misrepresentation, or the knowing concealment, suppression

or omission of any material fact with the intent that others rely upon such concealment, suppression or omission, in connection with the sale or advertisement of any merchandise or real estate, or with the subsequent performance of such person as aforesaid, whether or not any person has in fact been misled, deceived or damaged thereby..." N.J. STAT. ANN. § 56:8-2.

122. As set forth above, Facebook and Cambridge Analytica, while operating in New Jersey, engaged, in unconscionable commercial practices, deception, misrepresentation, and the knowing concealment, suppression, and omission of material facts with intent that others rely on such concealment, suppression, and omission, in connection with the sale and advertisement of services, in violation of N.J. Stat. Ann. § 56:8-2. This includes:

- a. Collecting, storing, and using vast quantities of highly sensitive personal information and which Facebook failed to adequately protect from unauthorized and/or criminal access;
- b. Failing to employ technology and systems to promptly detect unauthorized access to the personal information with which they were entrusted;
- c. Unreasonably delaying giving notice to consumers after it became aware of unauthorized access to the personal information;
- d. Knowingly and fraudulently failing to provide accurate, timely information to consumers about the extent to which their personal information had been compromised; and
- e. Making false and deceptive representations and communications concerning the purpose of and reasons for collecting highly sensitive personal information.

123. Facebook's and Cambridge Analytica's breach of their duties has directly and

proximately caused Plaintiffs and the New Jersey Subclass to suffer an ascertainable loss of money and property, including the loss of their personal information and foreseeably causing them to expend time and resources investigating the extent to which their personal information has been compromised.

124. The above unlawful and deceptive acts and practices and acts by Facebook and Cambridge Analytica were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiffs and the New Jersey Subclass that they could not reasonably avoid. This substantial injury outweighed any benefits to consumers or to competition.

125. Plaintiffs and the New Jersey Subclass seek relief under N.J. Stat. Ann. § 56:8-19, including, but not limited to, injunctive relief, other equitable actual damages (to be proven at trial), disgorgement of wrongfully obtained profits, treble damages, and attorneys' fees and costs.

SIXTH COUNT

Violation of California Business & Professions Code § 17200, *et seq.* (against Facebook and Cambridge Analytica)

126. Plaintiffs incorporate by reference the allegations in the preceding paragraphs as if fully set forth herein.

127. California Business and Professions Code Section 17200 prohibits any “unlawful, unfair or fraudulent act or practice....”

128. Facebook and Cambridge Analytica engaged in at least the following unfair or fraudulent acts or practices:

- a. Collecting, storing, and using vast quantities of highly sensitive personal information and which Facebook failed to adequately protect from unauthorized and/or criminal access;
- b. Failing to employ technology and systems to promptly detect unauthorized

- access to the personal information with which they were entrusted;
- c. Unreasonably delaying giving notice to consumers after it became aware of unauthorized access to the personal information;
 - d. Knowingly and fraudulently failing to provide accurate, timely information to consumers about the extent to which their personal information had been compromised; and
 - e. Making false and deceptive representations and communications concerning the purpose of and reasons for collecting highly sensitive personal information.

129. Facebook represented that it would not disclose users' personal information without consent and/or notice. It also required application developers, like Cambridge Analytica, to obtain and utilize users' personal information.

130. Cambridge Analytica obtained Plaintiffs' and Class members' personal information either wholly without authorization or in excess of any authorization it may have obtained.

131. Facebook's and Cambridge Analytica's conduct is also "unlawful" within the meaning of Section 17200 because it violated federal and state consumer protection and anti-fraud law.

132. The harm caused by Facebook's and Cambridge Analytica's conduct outweighs its utility, offends public policy, is immoral, unscrupulous, unethical, oppressive, deceitful, and offensive, and has caused and will continue to cause substantial injury to consumers, including Plaintiffs and members of the Classes.

133. Facebook and Cambridge Analytica had reasonably available alternatives to

advance its legitimate business purposes, such as using state-of-the-art technology and business practices to prevent the unauthorized access to the personal information, not using personal information without authorization or in excess of any authorization, and providing consumers with prompt, accurate, and fair notice of compromise to their personal information and redress.

134. Facebook's and Cambridge Analytica's breach of their duties has directly and proximately injured Plaintiffs and California Subclass, including the loss of their personal information and foreseeably causing them to expend time and resources investigating the extent to which their personal information has been compromised.

135. Plaintiffs and the California Subclass members seek relief under Section 17200, including damages (to be proven at trial), disgorgement of wrongfully obtained profits, attorneys' fees and costs, and injunctive relief.

SEVENTH COUNT

Violation of California Civil Code § 1798.80, *et seq.* (against Facebook)

136. Plaintiffs incorporate by reference the allegations in the preceding paragraphs as if fully set forth herein.

137. The California Customer Records Act ("CCRA") (Cal. Civ. Code § 1798.80, *et seq.*) ensures that "personal information about California residents is protected" by requiring any "business that owns, licenses, or maintains personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."

138. Plaintiffs and California Subclass are individuals protected by the CCRA.

139. Facebook is subject to the CCRA because it "owns, licenses, or maintains

personal information about [one or more] California resident[s].”

140. Facebook violated the CCRA because it failed to “implement and maintain reasonable security procedures and practices” to protect the personal information at issue from unauthorized access and, as a direct, proximate, and foreseeable result, the personal information of Plaintiffs and California Subclass was compromised.

141. Facebook further violated the CCRA by unreasonably delaying notification to Plaintiffs and California Subclass of the data breach.

142. Facebook breach of its statutory obligations has directly and proximately injured Plaintiffs and California Subclass, including the loss of their personal information and foreseeably causing them to expend time and resources investigating the extent to which their personal information has been compromised.

143. Plaintiffs and California Subclass are entitled to damages in an amount to be proven at trial, as well as other appropriate legal and equitable relief, plus attorneys’ fees and costs.

PRAAYER FOR RELIEF

WHEREFORE, Plaintiffs respectfully request, individually and on behalf of the alleged Classes and Subclasses, that the Court enter judgment in their favor and against Defendants as follows:

- A. An Order certifying each of the proposed Classes and appointing Plaintiffs and their Counsel to represent the Classes;
- B. An Order enjoining Facebook from engaging in the wrongful conduct alleged herein concerning disclosure and inadequate protection of Plaintiffs’ and Classes’ personal information;
- C. An Order compelling Facebook to employ and maintain appropriate systems and

policies to protect consumer personal information and to promptly detect, and timely and accurately report, any unauthorized access to that data;

D. An Order of disgorgement of wrongfully obtained profits;

E. An award of compensatory, statutory, and punitive damages, in an amount to be determined;

F. An award of reasonable attorneys' fees costs and litigation expenses, as allowable by law;

G. Interest on all amounts awarded, as allowed by law; and

H. Such other and further relief as this Court may deem just and proper.

JURY DEMAND

Plaintiffs demand, for themselves and each of the classes, a trial by jury, pursuant to the Federal Rules of Civil Procedure, of all issues so triable.

DATE: March 27, 2018

Respectfully submitted,

SEEGER WEISS LLP

By: /s/ Christopher L. Ayers
Christopher L. Ayers

Stephen A. Weiss
Christopher L. Ayers
SEEGER WEISS LLP
55 Challenger Road, 6th Floor
Ridgefield Park, New Jersey 07660
Telephone: (212) 584-0700
Facsimile: (212) 584-0799
E-mail: sweiss@seegerweiss.com
E-mail: cayers@seegerweiss.com

CARELLA, BYRNE, CECCHI,
OLSTEIN, BRODY & AGNELLO, PC

By: /s/ James E. Cecchi
James E. Cecchi

James E. Cecchi
Donald A. Ecklund
Michael A. Innes
CARELLA, BYRNE, CECCHI,
OLSTEIN, BRODY & AGNELLO, PC
5 Becker Farm Road
Roseland, NJ 07068-1739
(973) 994-1700
Email: jcecchi@carellabyrne.com
Email: decklund@carellabyrne.com
Email: minnes@carellabyrne.com

